

## Chapter 4: Integrality and some other things

Given a commutative ring  $R$ , we study  $R$ -algebras  $A$  so that  $A$  is finitely generated (or finite) as an  $R$ -module.

Examples:

1. The group ring  $RG$ . = free  $R$ -module with the elements of  $G$  as a basis. This is finite over  $R$  if  $G$  is finite.

2. Let  $R = \mathbb{Z}$  contained in the rational numbers  $\mathbb{Q}$ . What subrings are finitely generated as  $\mathbb{Z}$ -modules?

e.g., is  $\mathbb{Z}[\frac{1}{2}]$  finitely generated? No

The only such subring is  $\mathbb{Z}$ .

3. Inside  $\mathbb{Q}[i]$ , consider  $\mathbb{Z}[i]$ ,  $\mathbb{Z}[2i]$ ,  $\mathbb{Z}[i/2]$ .

$\mathbb{Z}[i]$  is finitely generated over  $\mathbb{Z}$ .  
 $\mathbb{Z}[2i] \subseteq \mathbb{Z}[i]$  is also finitely generated over  $\mathbb{Z}$ .  
 $\mathbb{Z}[\frac{i}{2}]$  is not fin. gen over  $\mathbb{Z}$ .

Defn. A commutative  $R$ -algebra  $A$  is finite over  $R$  if it is finitely generated as an  $R$ -module.

Does your neighbor know what an  $R$ -algebra is?

Yes ✓

No

Definition  $R$  is a commutative ring. An  $R$ -algebra  $A$  is a ring with a ring homomorphism  $\phi: R \rightarrow Z(A)$  (so  $1_R \mapsto 1_A$ ).  
 $A$  is an  $R$ -module via  $r \cdot a := \phi(r)a$ .

We learn:

- What condition on elements of  $A$  produce this finiteness condition
- What are the properties of integers.

Definitions. Let  $S$  be an  $R$ -algebra.

$S$  should be commutative.

An element  $s$  of  $S$  is **integral** over  $R$  if and only if

$p(s) = 0$  in  $S$  where  $p(x) \in R[x]$  is a monic polynomial.   
 monic; the leading coefficient is 1

The algebra  $S$  is integral over  $R$  if.

every element of  $S$  is integral over  $R$ .

Not clear:  $\mathbb{Z}\left[\frac{1+i\sqrt{3}}{2}\right] \subseteq \mathbb{C}$    
 is integral over  $\mathbb{Z}$ .

Examples:  $1 + i\sqrt{3}$  and  $(1+i\sqrt{3})/2$ .

$$(1+i\sqrt{3})^2 = 1 - 3 + 2i\sqrt{3} \\ = -2 + 2i\sqrt{3}$$

$$= 2(1+i\sqrt{3}) - 4$$

$1+i\sqrt{3}$  is a root of  $x^2 - 2x + 4$ .   
 so is integral over  $\mathbb{Z}$ .

$$\left(\frac{1+i\sqrt{3}}{2}\right)^2 = \frac{1+i\sqrt{3}}{2} - 1$$

$\frac{1+i\sqrt{3}}{2}$  is a root of  $x^2 - x + 1$    
 so is also integral over  $\mathbb{Z}$ .

$1+i\sqrt{5}$  is integral over  $\mathbb{Z}$    
  $\frac{1+i\sqrt{5}}{2}$  is not integral over  $\mathbb{Z}$ .

Goal: the integral elements form a sub ring. of  $S$ .

Corollary 4.6 plus. Let  $S$  be an  $R$ -algebra.

TFAE for  $s$  in  $S$

(a)  $s$  is integral over  $R$ .

(b)  $R[s]$  is contained in an  $R$ -submodule  $M$  of  $S$ , finitely generated over  $R$ , with  $sM \subseteq M$

(c) there exists an  $S$ -module  $N$  and a finitely generated  $R$ -submodule  $M$  of  $N$ , not annihilated by nonzero elements of  $S$ , such that  $sM \subseteq M$ .

Proof (a)  $\Rightarrow$  (b). Take  
 $M = R[s] (= \phi(R)[s])$   
 $\subseteq S$ .

Then  $s \cdot R[s] \subseteq R[s]$ .

Show  $R[s]$  is finitely generated over  $R$ . It is generated by

$$1, s, s^2, s^3, \dots$$

$$\text{If } p(s) = 0$$

$$p(x) = x^n + b_{n-1}x^{n-1} + \dots + b_0$$

$$\text{then } s^n = - (b_{n-1}s^{n-1} + \dots + b_0)$$

so  $s^n$  is not needed as a generator of  $R[s]$ . Neither are  $s^{n+1}, s^{n+2}, \dots$

$R[s]$  is generated by

$$1, s, s^2, \dots, s^{n-1} \quad \square$$

(b)  $\Rightarrow$  (c): In (c) take  $N = S$   
 $M$  the same. Then  $1 \in R[s] \subseteq M$   
is not ann. by any non-zero elt of  $S$ .

$\square$

# Pre-class Warm-up!!!

Is 2 integral over  $\mathbb{Z}$  ?

A Yes ✓

B No

Is  $1/2$  integral over  $\mathbb{Z}$  ?

A Yes

✓

Some further questions we might discuss (or not!)

Is  $\mathbb{Z}[x] / (2x^3)$

(a) finitely generated as a ring? Yes

(b) finitely generated as an abelian group? No

Degree	0	1	2	3	4	5
elements	1	$\bar{x}$	$\bar{x}^2$	$\overline{\mathbb{Z}x^3}$		
	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z} \cong \mathbb{Z} \cong \mathbb{Z}$	$\mathbb{Z} \cong \mathbb{Z} \cong \mathbb{Z}$	$C_2$	$C_2$

Another question: (a) and (b) for  $\mathbb{Z}[x]/(x^3)$ .

Yes and Yes.

Goal: the integral elements form a sub ring.

Corollary 4.6 plus. Let  $S$  be an  $R$ -algebra.

TFAE for  $s$  in  $S$

(a)  $s$  is integral over  $R$ .

(b)  $R[s]$  is contained in an  $R$ -submodule  $M$  of  $S$ , finitely generated over  $R$ , with  $sM \subseteq M$

(c) there exists an  $S$ -module  $N$  and a finitely generated  $R$ -submodule  $M$  of  $N$ , not annihilated by nonzero element of  $S$ , such that  $sM \subseteq M$ .

(c)  $\Rightarrow$  (a) Let  $M = Rm_1 + \dots + Rm_n$   
 $m_i \in M$ . Let  $s$  satisfy  $sM \subseteq M$

Write  $sm_i = \sum a_{ij} m_j$

$a_{ij} \in R$ , for each  $i$ .

Let  $A = (a_{ij})$

Now  $(A - sI) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$

$$\text{adj}(A - sI)(A - sI) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \text{adj}(A - sI) \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$= \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\det(A - sI) \cdot I \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\det(A - sI) m_i = 0$$

$$\text{so } \det(A - sI) \cdot M = 0$$

$$\text{and } \det(A - sI) = 0.$$

If  $p(t) = \det(A - tI)$  then  
 $p$  is monic and  $p(s) = 0$ .

$s$  is integral over  $R$ .  $\square$

$\det \begin{bmatrix} a_{11} - s & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - s & \dots & \dots \\ \dots & \dots & \dots & \dots \\ \dots & \dots & \dots & \dots \end{bmatrix}$  is monic.

Theorem 4.3 (Cayley-Hamilton) *commutative*.

Let  $\mathcal{I}$  be an ideal of a ring  $R$ ,  
 $M$  an  $R$ -module generated by elements  
 $m_1, \dots, m_n$ ,

$f: M \rightarrow M$  an endomorphism. *of  $R$ -modules*.

If  $f(M) \subseteq \mathcal{I}M$  *JM*

then there is a polynomial

$$p(x) = x^n + p_1 x^{n-1} + \dots + p_n$$

so that  $p(f) = 0$ , with  $p_j \in \mathcal{I}^j \forall j$ .

*Proof.* Write  $f(m_i) = \sum a_{ij} m_j$ ,  $a_{ij} \in \mathcal{I}$

Let  $A = (a_{ij})$

Regard  $M$  as an  $R[x]$ -module with  
 $x$  acting as  $f$ .

$$\text{Now } (xI - A) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = 0$$

*elements of  $M$  i.e. vectors. Not allowed.*

$$\text{adj}(xI - A) \cdot (xI - A) \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

$$\det(xI - A) \mathcal{I} \begin{bmatrix} m_1 \\ \vdots \\ m_n \end{bmatrix} = \begin{bmatrix} 0 \\ \vdots \\ 0 \end{bmatrix}$$

If  $p(x) = \det(xI - A)$  then

$p(x) \cdot M = 0$ , so  $p(f) = 0$ .  $\square$

and  $p_j \in \mathcal{I}^j$ .

*adj  $B \cdot B = \det(B) \cdot I$   
Math 4242: entries of  $B$   
are in a field.*

Questions:

1. Could we present this proof to  
undergraduates in Math 4242? Why, or why  
not? *Yes*

*No Most*

2. How many points in this proof are  
troubling to you?

0 1 2 3 4

# Pre-class Warm-up

Let  $R$  be a subring of  $S$ ,  $u$  an element of  $S$  and  $r$  an element of  $R$ .

Is it obvious that if  $u$  is integral over  $R$  then  $ru$  is also integral over  $R$ ?

A Yes

B No

$$u^n + a_{n-1}u^{n-1} + \dots + a_0 = 0$$

$$r^n u^n + r^n a_{n-1} u^{n-1} + \dots + r^n a_0 = 0$$

$$(ru)^n + r a_{n-1} (ru)^{n-1} + \dots = 0$$

Corollary = Theorem 4.2.

Elements of  $S$  integral over  $R$  form an  $R$ -subalgebra.

Proof. We show if  $a, b \in S$  are integral over  $R$  then so are  $a+b, ab$ .

$a \in M \subseteq S$ ,  $M$  is fin gen as an  $R$ -module  $aM \subseteq M$ .

Similarly  $b \in M' \subseteq S$  <sup>same conditions.</sup>

If  $M$  is gen'd over  $R$  by

$m_1, \dots, m_u$

$M'$   $\dots$

$m'_1, \dots, m'_v$

then  $MM' = \{mm' \mid m \in M, m' \in M'\}$   
 $\subseteq S$

is an  $R$ -module generated by the  $m, m_j$ .

$$abMM' = aM bM' \subseteq MM'$$

$$(a+b)MM' \subseteq aMM' + bMM'$$

$$\subseteq MM' + MM' = MM'$$

Thus  $ab, a+b$  satisfy the criterion to be integral over  $R$ .  $\square$

Why do we go through this elaborate process to show this?



Proposition 4.1. Let  $R$  be a ring,  $J$  an ideal of  $R[x]$ ,  $S = R[x]/J$ .

Let  $s$  be the image of  $x$  in  $S$ .

a.  $S$  is generated by  $\leq n$  elements as an  $R$ -module if and only if  $J$  contains a monic polynomial of degree  $\leq n$ .

In this case  $S$  is generated by  $1, s, s^2, \dots, s^{n-1}$ .

b.  $S$  is a finitely generated free  $R$ -module if and only if  $J$  can be generated by a monic polynomial.

In this case  $S$  is freely generated by  $1, \dots, s^{n-1}$  where  $n = \text{degree of that polynomial}$ .

Proof a. " $\Leftarrow$ " If  $J \ni p$  a monic polynomial of degree  $n$

$$p(x) = x^n + a_{n-1}x^{n-1} + \dots + a_0$$

$$\text{then } x^n = -(a_{n-1}x^{n-1} + \dots + a_0)$$

so  $s^n$  lies in the sub  $R$ -module generated by  $1, \dots, s^{n-1}$ .

Example.  $R = \mathbb{Z}$ ,  $J = (2x^3)$

$R[x]/J$						
degree	0	1	2	3	4	...
	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	$\mathbb{Z}/2\mathbb{Z}$	...

This is not finitely generated as a  $\mathbb{Z}$ -module.

so does  $s^{n+1}$  etc.

" $\Rightarrow$ " If  $S$  is generated by  $m_1, \dots, m_n$  Cayley-Hamilton  $\Rightarrow s$  is a root of a monic  $p(x)$  of degree  $n$ .  $p \in J$ .  $\square$

$$e \in S \supseteq R$$

Corollary.  $s$  is integral over  $R$  if and only if  $R[s]$  is finitely generated as an  $R$ -module.

Proof. " $\Rightarrow$ "  $s$  integral  $\Rightarrow$   
 $p(s) = 0$ ,  $p \in R[x]$  monic,  
 $R[s] \cong R[x]/(p)$  is  
finitely generated over  $R$ .

" $\Leftarrow$ " Use Cor 4.6 with  
 $M = R[s]$ .  $\square$

Corollary 4.4. Let  $M$  be a finitely generated  $R$ -module.

a. If  $f: M \rightarrow M$  is an epimorphism of  $R$ -modules, then  $f$  is an isomorphism.

Proof. Apply Cayley-Hamilton.

Take the ring to be  $R[x]$ .

Let  $M$  be an  $R[x]$ -module where  $x$  acts via  $f$ .

( $xm := f(m)$ ).

Take the ideal  $I$  to be  $(x)$ .

Then  $f: M \rightarrow M$  has image in  $IM = M$  so  $1_M$  satisfies

$$p(t) = t^n + a_{n-1}t^{n-1} + \dots + a_0$$
$$p(1) = 0$$

$$a_i \in I' \subseteq I$$

$$1 + f \cdot q = 0$$

because  $a_{n-1}t^{n-1} + \dots + a_0$  is divisible by  $x$ .

$$fq = -1 \quad f(-q) = 1$$

$f$  is invertible,  $\square$

Corollary 4.5.

An  $R$ -algebra  $S$  is finite over  $R$  if and only if  $S$  is generated as an  $R$ -algebra by finitely many integral elements.

## 4.2 Normal domains

Definition. Let  $R$  be an integral domain. Then  $R$  is normal if and only if it equals its own integral closure in its field of fractions.

Examples  $\mathbb{Z}[i\sqrt{3}]$  is not normal

$\mathbb{Z}[i\sqrt{5}]$  is normal

Proposition 4.10

Let  $R$  be a ring. If  $R$  is factorial, then  $R$  is normal.

The extra things in Eisenbud's book:



## Nakayama's Lemma

First a lemma coming from the Cayley-Hamilton theorem again:

### Corollary 4.7

Let  $M$  be a finitely generated  $R$ -module,  $J$  an ideal of  $R$  so that  $JM = M$ .

Then there is an element  $r$  in  $J$  that acts as the identity on  $M$ ; i.e.  $(1-r)M = 0$ .

Definition. The Jacobson radical of a ring  $R$  is the intersection of the maximal ideals of  $R$ .

Examples.

### Corollary 4.8 (Nakayama's lemma)

Let  $J$  be an ideal contained in the Jacobson radical of  $R$ , let  $M$  be a finitely generated  $R$ -module

a. If  $JM = M$  then  $M = 0$ .

b. If  $m_1, \dots, m_n$  in  $M$  have images in  $M/JM$  that generate it as an  $R$ -module then these same elements generate  $M$  as an  $R$ -module